Aalto University

International Seminar on Safety and Security of Autonomous Vessels
17 - 18 September 2019, Helsinki

Safety related cyber-attacks identification and assessment for autonomous inland ships

Victor Bolbot[1*], Gerasimos Theotokatos[1], Evangelos Boulougouris[1] and Dracos Vassalos
[1] Maritime Safety Research Centre, University of Strathclyde, UK

ABSTRACT

Recent advances in the maritime industry include the research and development of new sophisticated ships including the autonomous ships. The new autonomy concept though comes at the cost of additional complexity introduced by the number of systems that need to be installed on-board and on-shore, the software intensiveness of the complete system, the involved interactions between the systems, components and humans and the increased connectivity. All the above results in the increased system vulnerability to cyber-attacks, which may lead to unavailability or hazardous behaviour of the critical ship systems. The aim of this study is the identification of the safety related cyber-attacks to the navigation and propulsion systems of an inland autonomous ship as well as the safety enhancement of the ship systems design. For this purpose, the Cyber Preliminary Hazard Analysis method is employed supported by the literature review of the system vulnerabilities and potential cyber-attacks. The Formal Safety Assessment risk matrix is employed for ranking of the hazardous scenarios. The results demonstrate that a number of critical scenarios can arise on the investigated autonomous vessel due to the known vulnerabilities. These can be sufficiently controlled by introducing appropriate modifications of the system design.

Keywords: Safety; Cybersecurity; Autonomous inland vessel; Navigation and propulsion systems; Cyber Preliminary Hazard Analysis.

1 INTRODUCTION

Cyber-Physical Systems (CPSs) represent a class of systems consisting of control elements as well as software and hardware, which are used to effectively control physical processes advancing in a number of application areas including the maritime industry (DNV GL, 2015). CPSs are expected to increase the productivity and safety levels by removing, substituting and/or supporting the operator in the decision-making process, thus reducing the number of human errors leading to accidents. Typical examples of the marine CPSs include the Diesel-Electric Propulsion plant, the Safety Monitoring and Control System, the Dynamic Positioning System as well as the Heating Ventilation Air Conditioning systems (DNV GL, 2015). The number of the CPSs is expected to increase in autonomous ships, which are considered to be the ultimate maritime CPS.

The introduction of the CPSs is accompanied with increased complexity owed to the heterogeneous character of the CPSs, the dependence on information exchanging with other systems, the additional new interactions with humans, the increased number of controllers running complicated software and the increased interconnectivity required for implementing the desired CPSs' functionalities (Bolbot, Theotokatos, Bujorianu, Boulougouris, & Vassalos, 2019). However, this also introduces new hazards as cyber-attacks can exploit vulnerabilities in the communication links and directly affect the integrity or availability of the data and control systems leading the CPSs

* Corresponding author: victor.bolbot@strath.ac.uk

to accidents (Bolbot et al., 2019; Eloranta & Whitehead, 2016). Considering that ships and their cargo are assets with great value, this inevitably will lead to severe financial consequences in case of an autonomous vessel; it may also have serious safety implications.

There is an increasing number of concerns with respect to the ship systems vulnerability to cyber-attacks in the maritime industry and a number of guidelines have been developed to address these concerns (Boyes & Isbell, 2017; DNV GL, 2016, 2019; IMO, 2016; Maritime affairs directorate of France, 2016; United States Coast Guard, 2015). In addition, a number of previous research studies focused on the cyber security assessment of the ship control systems and ship networks in autonomous ships. Jones, Tam, and Papadaki (2016) reported the identification of different attack scenarios on a cargo ship. Tam and Jones (2019) proposed a model-based approach for the risk assessment of cyber-threats named MaCRA (Maritime Cyber-Risk Assessment) by considering the technological systems vulnerabilities as well as the ease-of-exploit and the potential hackers rewards. Using the same model-based approach, Tam and Jones (2018) implemented a risk assessment for a number of autonomous vessels. Kavallieratos, Katsikas, and Gkioulos (2019) employed the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege) method to assess risks in an autonomous vessel. Omitola, Downes, Wills, Zwolinski, and Butler (2018) analysed an unmanned surface vessel navigation system using the System-Theoretic Process Analysis for cyber-attacks (STPA-sec) targeting at modifying data that are provided as input to the vessel navigation system.

However, in the previous research studies the risk assessment was implemented considering high level system architecture. Furthermore, the risk assessment in the previous studies identified a number of potential attack scenarios, but did not focus on the safety related consequences. In addition, none of the previous studies conducted a risk assessment of an inland autonomous vessel. Inland autonomous vessel is operating in different environment from the short sea or ocean going vessels, has different system requirements and size and can attract the interest from different hackers groups than the short sea and ocean going vessels.

Therefore, the hazardous scenarios that can arise due to cyber-attacks can be very different in autonomous inland ship. In this respect, the aim of this study is to implement a risk assessment for the navigation and propulsion systems of an inland autonomous vessel. To the best of authors knowledge, this is the first study applying the Cyber Preliminary Hazard Analysis (CPHA) method to an autonomous vessel. The novel contributions of the study include (a) the adjustment of CPHA for application to ship systems, (b) the identification of potential hazardous scenarios arising due to cyber-attacks in propulsion and navigation system of an inland autonomous ship and (c) the highlighting of the critical safety/cyber security control measures for this ship.

The remaining of this paper is organised as follows. The followed method for cyber-attacks risk assessment is presented in Section 2. A description of an inland autonomous vessel navigation and propulsion systems is provided in section 3. In section 4, the results of the method application are provided and discussed. In the conclusions section, the main findings are summarised and suggestions for the future research are provided.

2 METHODOLOGY

During the selection of suitable methods, the following requirements have been considered:

- The method must be aligned with the relevant cyber security standards - IEC 62443, ISO 27000 and IEC 61580, and need to be applicable either during the high-level or the detailed level risk analysis (Flaus, 2019).
- The method must focus on the cyber security induced safety risks (Flaus, 2019).
- The method must incorporate different potential attackers groups (Tam & Jones, 2019).
- The method must be marinised – addressing the needs of maritime industry and aligned with the maritime regulations for safety approval (International Maritime Organisation, 2013).
- The method must be preferentially model-based (Bolbot et al., 2019).

Based on the above considerations the Cyber Preliminary Hazard Analysis (CPHA) (Flaus, 2019) has been selected. The advantages of this method are the following:

- The method can be applied during the initial design stages and does not require many details for the investigated system characteristics (Bolbot et al., 2019) similarly with the STRIDE and MaCRA methods.
- The method is not as labour intensive as STPA (Abdulkhaleq & Wagner, 2015), although it can be less formal approach and less detailed when it comes to hazards identification. Therefore, the CPHA is easier to be applied during high-level risk assessment. The STPA does not have any specific guidance related to identification of cyber attacks, simply suggests that some hazardous scenarios can arise due to cyber security violation (Young & Leveson, 2014). The CPHA also allows ranking of different scenarios which is not integral part of the STPA.
- The method incorporates the available or new safety and security barriers, guiding in this way the system design improvement. This information is not present in the STRIDE and MaCRA methods.
- Compared to the STRIDE and MaCRA methods, the CPHA: (a) is not limited to the specific suggested attack types, and; (b) describes better the relevant hazardous scenarios by incorporating the potential attack type and the relevant hazardous consequences.
- CPHA is based on Preliminary Hazard Analysis (PHA), which is a well-known method for safety assessment and is proposed by ISO 31000 and IEC 61580.

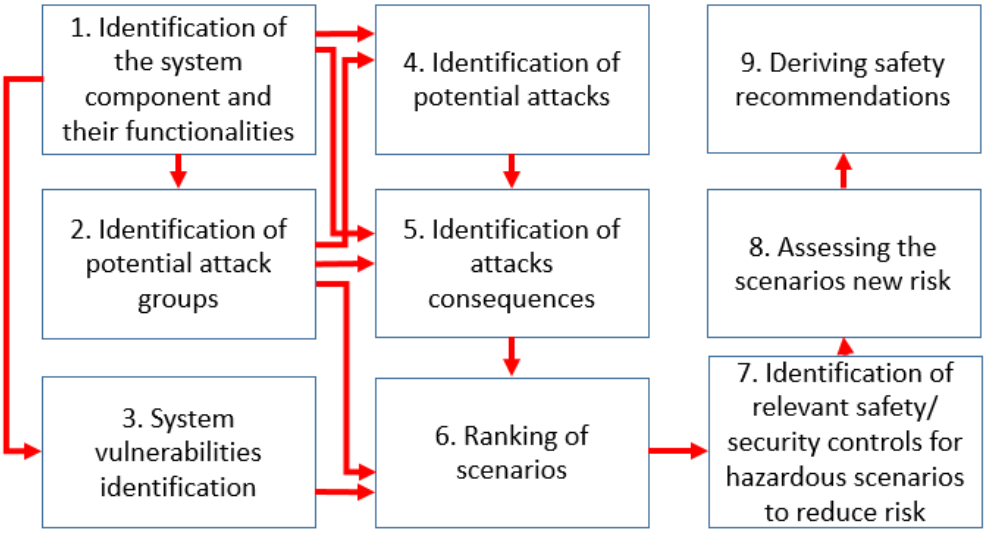

Figure 1 CPHA methodology flowchart.

The CPHA followed steps are provided in the flowchart depicted in Figure 1, whilst the method steps are elaborated further below. These are the CPHA steps described in (Flaus, 2019) with small modifications. Another difference is that the scenarios ranking is implemented using Formal Safety Assessment risk matrix (International Maritime Organisation, 2013).

The prerequisite for the CPHA is the identification of: (a) the control system elements, (b) the control system elements interfaces with the physical word, the controlled processes and other control system elements interfaces, (c) the potential entry points into system. This is implemented in step 1 (Figure 1), by analysing the available system information as well as by developing the system physical and logical mapping (Flaus, 2019).

As the attackers do not have neither the same motives nor the same resources when attacking a ship network (Tam & Jones, 2019), for identifying and ranking the attack scenarios in step 5 (Figure 1), the following parameters need to be considered: (a) which entry points can be exploited, and; (b) which system will be targeted and (c) in which way by each attacker group. In this respect, the potential attack groups are identified in step 2 (Figure 1) by referring to the relevant literature.

The known vulnerabilities and the potential entry points are identified in step 3 (Figure 1) by using the information provided in the following resources: (a) previous research publications e.g. (Flaus, 2019; Kavallieratos et al., 2019; Omitola et al., 2018; Tam & Jones, 2018); (b) the available maritime standards (Boyes & Isbell, 2017; DNV GL, 2016; IMO, 2016; Maritime affairs directorate of France, 2016); (c) relevant generic standards (IEC, 2011a), and; (d) the Cybersecurity and Infrastructure Security Agency (CISA) database (CISA, 2019a).

The potential vulnerabilities in the system are used to develop the potential attack scenarios in step 4 (Figure 1) (Flaus, 2019). The information about the system interactions and system components functionalities is used to derive the potential consequences in step 5 (Figure 1). In step 6, the scenarios are ranked according to the expected frequency occurrence and the severity of consequences. The frequency and the severity of each attack scenario are ranked using the Formal Safety Assessment (FSA) suggested ranking tables (International Maritime Organisation, 2013), presented in Table 1 and Table 2, whilst the risk is evaluated using the risk matrix presented in Table 3 to harmonise the analysis results with the relevant IMO Formal Safety Assessment guidelines. The frequency ranking for each attack scenario is implemented by considering (a) the level of exposure of each system to attack due to connectivity, (b) the interest of specific attack group in an attack scenario, (c) the attacker level and (d) the access control to the systems. The severity ranking is implemented based on consequences. The preventive and mitigating barriers are identified and proposed in step 7. Then, the scenarios risk is reassessed considering the available or the preventive and mitigating barriers. Based on this analysis results, the relevant safety recommendations at the initial ship design stage are derived. These results can be used as input to more detailed analysis as required by IEC 62443 (BSI, 2009).

Table 1 Ranking for successful attack scenarios (International Maritime Organisation, 2013).

Ranking (FI)	Frequency	Definition	F (per ship year)	F (per ship hour)
7	Frequent	Likely to occur once per month on one ship	10	$1.14\ 10^{-3}$
5	Reasonably probable	Likely to occur once per year in a fleet of 10 ships, i.e. likely to occur a few times during the ship's life	10^{-1}	$1.14\ 10^{-5}$
3	Remote	Likely to occur once per year in a fleet of 1,000 ships, i.e. likely to occur in the total life of several similar ships	10^{-3}	$1.14\ 10^{-7}$
1	Extremely remote	Likely to occur once in the lifetime (20 years) of a world fleet of 5,000 ships.	10^{-5}	$1.14\ 10^{-9}$

Table 2 Ranking for severity of consequences (International Maritime Organisation, 2013).

Ranking (SI)	Severity	Effects on human safety	Effects on ship	Oil spillage definition	S Equivalent fatalities
4	Catastrophic	Multiple fatalities	Total loss	Oil spill size between < 100 - 1000 tonnes	10
3	Severe	Single fatality or multiple severe injuries	Severe damage	Oil spill size between < 10 - 100 tonnes	10^{-0}
2	Significant	Multiple or sever injuries	Non-severe ship damage	Oil spill size between < 1 - 10 tonnes	10^{-1}
1	Minor	Single or minor injuries	Local equipment damage	Oil spill size < 1 tonne	10^{-2}

Table 3 The risk matrix (International Maritime Organisation, 2013)

Risk Index (RI)					
FI	Frequency	Severity (SI)			
		1	2	3	4
		Minor	Significant	Severe	Catastrophic
7	Frequent	(H) 8	(H) 9	(H) 10	(H) 11
6		(M) 7	(H) 8	(H) 9	(H) 10
5	Reasonably probable	(M) 6	(M) 7	(H) 8	(H) 9
4		(M) 5	(M) 6	(M) 7	(H) 8
3	Remote	(L) 4	(M) 5	(M) 6	(M) 7
2		(L) 3	(L) 4	(M) 5	(M) 6
1	Extremely remote	(L) 2	(L) 3	(L) 4	(M) 5
High (H) =Intolerable Risk		Medium (M) =Tolerable Risk		Low (L) =Negligible Risk	

3 CASE STUDY DESCRIPTION

The proposed methodology was applied to an autonomous version of a conventional operational Pallet Shuttle Barge (PSB) (Blue Lines Logistics, 2015) as the particular PSB is going to be retrofitted into an autonomous during AUTOSHIP project. The selected autonomous PSB is supposed to operate from/to the port of Antwerp in Belgium and the interconnected canals. The main ship particulars are provided in Table 4. The focus of the analysis was put on this vessel navigation and propulsion systems, as they are considered the most vulnerable to cyber-attacks (BIMCO, 2018). The equipment that is used for the navigation and the propulsion, as well as the relevant interconnections and interactions between the involved subsystems are schematically shown in Figure 2. The network description was developed based on the information provided in (Boyes & Isbell, 2017; Höyhtyä, Huusko, Kiviranta, Solberg, & Rokka, 2017; Maritime affairs directorate of France, 2016; Schmidt, Fentzahn, Atlason, & Rødseth, 2015; Stefani, 2013) and available drawings for similar ships. The actual network interconnections and equipment may differentiate in the final design of this autonomous PSB. The PSB selected components functionalities description is provided in Table 5. For the present analysis, it was considered that the PSB is in fully autonomous operation, so there is no crew onboard the vessel.

Table 4 PSB particulars.

Type	Catamaran
Length	50 m
Breadth	6.6 m
Maximum Draught	2.2 m
Air draught	5.6 m
Maximum cargo load	300 tonnes
Maximum speed	8.1 knots
Engine output	300 hp
Propulsion type	Diesel-mechanical with azimuth propulsion aft and bow thruster at the bow

Table 5 PSB selected components functionalities description.

Component	Functions
Shore control centre	• Monitoring of physical processes • Navigation control • Control over the ship in emergency/manoeuvring operating modes • Implementation of software updates
Connectivity manager	• Control over information flow between the vessel and the shore control centre
Autonomous ship controller	• Monitoring of the processes safety and alarm generation • Control over ship operating modes (emergency, sailing, autonomous, remotely controlled etc.)
Ship control station	• Interface between crew on board and the vessel, allowing the crew to take control over the navigation systems and engine automation systems
Engine automation system	• Machinery components health monitoring
System Control And Data Acquisition (SCADA) server	• Machinery system sensors measurements and alarms data log
Main engine controller	• Control over engine speed • Engine health status monitoring
Generator controller	• Generator speed control • Generator health status monitoring
Azimuth controller	• Azimuth angle control • Azimuth health monitoring
Bow thruster controller	• Bow thruster speed control
Network cabinet	• Interconnection with other systems
Route planning system	• Selecting the route between departure and arrival point based on the traffic in area
Navigation and collision avoidance system	• Navigating within ports and channels • Position holding • Avoiding collision with other vessels and objects
Situation awareness system	• Picture compilations around the vessel
Electronic Chart Display Information System (ECDIS)	• Detecting position of the ship on the map
Voyage Data Recorder (VDR)	• Principal alarms and sensors measurements recording
Very High Frequency (VHF) radio	• Transmitting messages between vessels
Automatic Identification System (AIS)	• Sending and receiving GPS positions, speed, heading, type of ship, next port and estimated time of arrival to and from surrounding ships
Global Maritime Distress and Safety System (GMDSS)	• Sending and receiving critical safety alerts
RAdio Detection And Ranging (RADAR)	• Detection and determination of the position and speed of the objects
Light Detection And Ranging (LiDAR)/ Laser Detection And Ranging (LADAR)	• Detection and determination of the position and speed of the objects with greater accuracy
Video cameras	• Objects detection and recognition
Echo sounder	• Depth measurement
Global Positioning System (GPS)	• Position measurement, and indirectly speed measurement
Gyro compass	• Angular position and velocity measurement
Speed log measurement	• Speed measurement

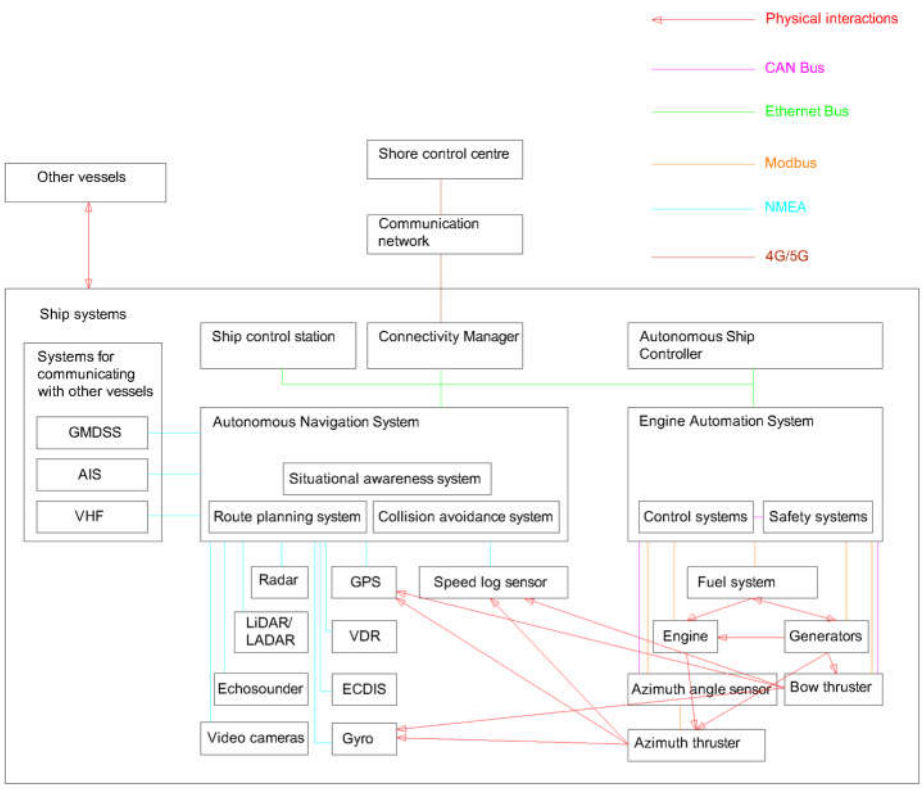

Figure 2 Schematic of PSB network and interactions

4 RESULTS AND DISCUSSION

The investigated autonomous ship systems control elements, their interactions with other control elements, the potential entry points and the relevant network zones are presented in Figure 2 and Figure 3, which are the results of the used methodology first step.

The potential attackers can be classified into the following groups (Results of step 2) (Boyes & Isbell, 2017; Flaus, 2019; IEC, 2011b; Tam & Jones, 2019):

- Former malicious employees aiming at taking revenge from the ship operating company.
- Malicious external providers desiring to steal the machinery data.
- Activists opposed to autonomous ships introduction in the maritime industry (Hacktivists).
- Hackers willing to prove and train their skills.
- Competitors aiming at stealing valuable data or sabotaging and damaging the ship.
- Criminals aiming at stealing the ship, its cargo, components or seeking for a monetary reward.
- Terrorists aiming at damaging the ship and/or causing fatalities.
- States in case of total war aiming at damaging or taking control over the ship.

Since the terrorist group is the group of people targeting the most on the accident achievement, the focus of the present case study will shift towards identifying attacks and safety scenarios, which may be of interest by terrorists. For this analysis, it was assumed that there is an undisclosed group of terrorists which possesses significant technical knowledge about the vessel and its communication systems. This group attacks can be considered similar to the attacks implemented by states in case of a total war. The potential vulnerabilities that can be exploited and the attacks that can be realised are provided in the following paragraphs.

Social engineering attacks are considered the most powerful tool on the hackers hands (Flaus, 2019). Thus, a successful phishing scam can be used to get access of the ship through the shore control centre. Attacks installing malware using flash medium can be also implemented on the shore

control centre and at ship control station, as described in (Lund, Hareide, & Jøsok, 2018) or through accidental communication bridges developed between the smart devices with wireless connectivity used by maintenance personnel and the ship control systems (Oates, Roberts, & Twomey, 2017). 4G protocol has been found vulnerable to a number of attacks, where a malicious node can be used to impede the communication or to steal information (Hussain, Chowdhury, Mehnaz, & Bertino, 2018). However the ship satellite communications systems have been also proved to be vulnerable to penetration (Munro, 2017). Configurations in the communication between the ship and the shore control centre including an anonymous File Transfer Protocol can lead to a cyber security breach (IEC, 2011b). Even Virtual Private Networks can have exploitable vulnerabilities, such as the use of outdated communication protocols (DNV GL, 2016; Flaus, 2019). Remote access can be also facilitated by using an available web link to the system equipment with inappropriate username and password (Munro, 2017; Oates et al., 2017) or due to inappropriate remote unit firewall configuration settings (CISA, 2019d; DNV GL, 2016; Oates et al., 2017).

Physical attacks (Flaus, 2019) can be also considered in the case of PBS as the vessel is operating in a close proximity to the shore (or river/channel banks) and no crew is present. The Programming Logic Controllers (PLCs) can be vulnerable to Denial of Service (DoS) or malware attacks due to an unchecked integer overflow vulnerability (Flaus, 2019) or other vulnerabilities (CISA, 2019b; Oates et al., 2017). Considering that patching may not be as frequently implemented as required and that due to the extensive ship lifetime compared to other information technology systems it may not be technically feasible to patch the software (Oates et al., 2017). Therefore it is highly likely that known vulnerability is being exploited (Nazir, Patel, & Patel, 2017; Oates et al., 2017). However system patching by system provider itself opens new opportunities for attacks as it requires remote connection to the vessel and can allow malware propagation from the software owner (Oates et al., 2017). System hardware can be already infected with malware installed before actual installation on the ship (logic bombs and backdoors) which cannot be captured by functional testing (Oates et al., 2017). An attacker can even freeze one sensor measurement in a PLC, misleading in this way the operator (Krotofil et al., 2014). It is even possible to modify the sensor measurement and trigger a faulty safety alarm (Shinohara & Namerikawa, 2017). The navigation computer systems can be infected using SQL injections (DNV GL, 2016; Flaus, 2019) and the ship navigation systems have been proved vulnerable to malware installations (Wingrove, 2018).

GPS signal is a relatively weak signal and can be easily jammed (Borio, Driscoll, & Fortuny, 2012; Boyes & Isbell, 2017; Farid, Ahmad, Ahmed, & Rahim, 2018), spoofed (Goward, 2017) or resent with delay (Omitola et al., 2018) . AIS information is transferred using VHF radio with no encryption allowing valuable information to be easily obtained (Maritime affairs directorate of France, 2016) but it can be also altered or jammed (Balduzzi, Pasta, & Wilhoit, 2014). LiDAR sensors depend on reflection signal, so they can be spoofed if objects with relevant reflective/absorbent surfaces are set in front of them (Brooks, 2016). Cameras can be easily dazzled or spoofed as well (Alguliyev, Imamverdiyev, & Sukhostat, 2018; Brooks, 2016). The components connected to CAN networks are vulnerable to Denial of Service (DoS) attacks, as an artificial control node can be created in the network, shadowing other controllers, sensors and actuators (Bozdal, Samie, & Jennions, 2018; Kang, Song, Jeong, & Kim, 2018). This generates opportunities for attacks if a physical device can be attached to the ship CAN (CISA, 2019c). Modbus protocol is among the oldest protocols, which is not encrypted and a DoS attack can be easily implemented affecting in this way the availability of sensors/actuators (Flaus, 2019).

More vulnerabilities can be found on Cybersecurity and Infrastructure Security Agency (CISA) website (CISA, 2019a) and National Vulnerability Database (NIST, 2019). For the present analysis though, the above list of vulnerabilities can be considered as adequate.

The CPHA scenarios with RI greater or equal with 9 (Steps 4-8 in Figure 1) are provided in Table 6. In total 48 scenarios have been identified, with 19 of them being critical, 24 in a tolerable region and only 5 of them have been initially characterised as negligible. After the incorporation of the available and new safety/cyber security/security barriers, no scenarios were considered as critical, 21 were considered as tolerable and the rest (27) as negligible. The most critical scenarios are related to the access to the ship control station and shore control station, whilst other top critical

ones were related either to the GPS signal related attacks or a malware installation on the collision avoidance system and the situation awareness system. In this analysis, single attacks scenarios have been considered. However, more complicated attacks can be implemented, if several single attack scenarios are combined. Their identification is a subject of detailed risk analysis and hence out of the scope of the present research.

The suggested safety cyber security recommendations (step 9 Figure 1) include the following:

- Increasing redundancy in communication between different network zones (Zone 1, Zone 2, Zone 3 and Zone 4).
- Installation of firewalls between each zone (on the conduits).
- Addition of a safety system verifying the safety of the automatic navigation control system actions.
- Sanity checks and filter application for the GPS signals measurements, addition of anti-interference antennas.
- Encryption for the VHF signals.
- Use of kernels on the critical controllers.
- Two or three factors authentication for software updates and patching.
- Installation of an intrusion detection system in each zone.
- Selecting critical health sensor measurements and sending them to the shore control centre at specific intervals.
- Implementing a safe system shutdown, in case of a critical systems loss.
- Interconnecting the main engine with the generator using power take-in/take off systems.
- Plan route verification by the shore control centre

.

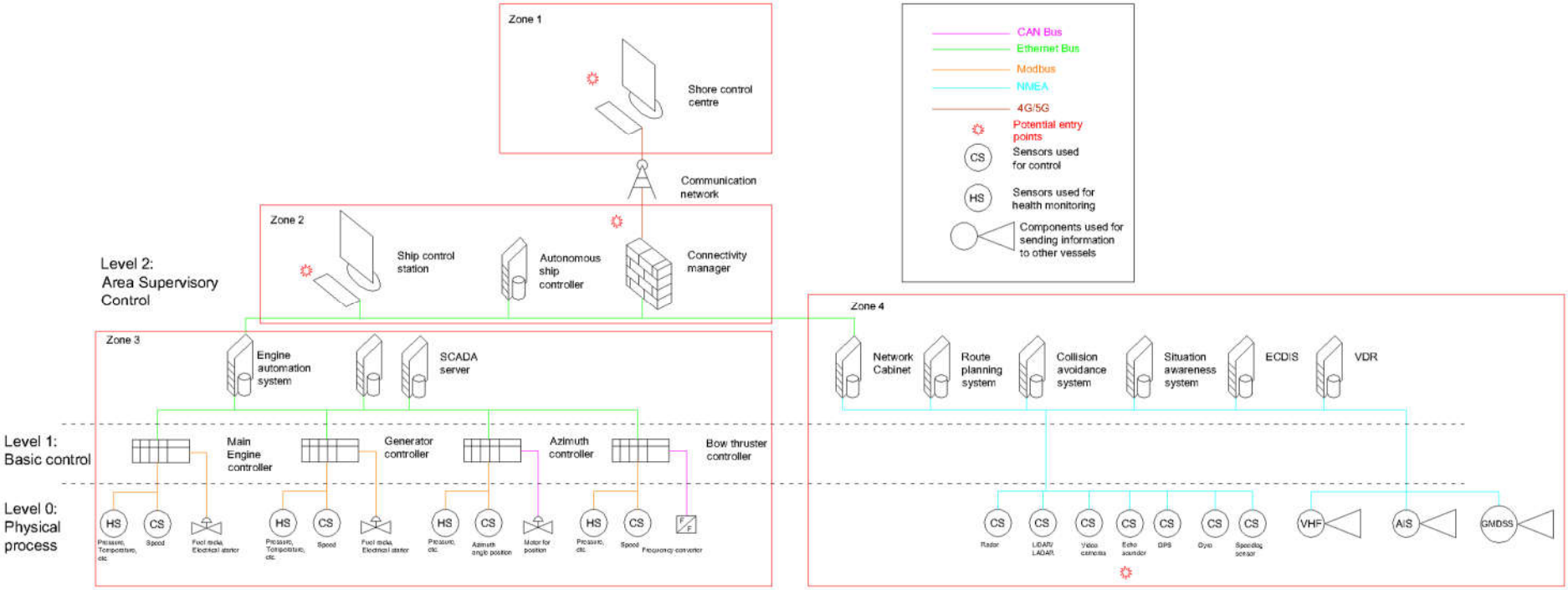

Figure 3 Network logical modelling.

Table 6 The critical CPHA scenarios (initial risk greater or equal than 9).

a/a	System	Attack	Feared event	Consequences	FI	SI	RI=S+SI	Safety/security barriers	S2	SI2	R2=S2+SI2
1	Shore control centre	Social engineering	Stealing access data and gaining authority to perform modifications	Malware installation on ship and loss of ship control	5	4	9	Isolation of shore control centre from the company business network / Closing USB ports / Advanced intrusion detection systems and Antivirus	3	4	7
8	Ship control station	Physical attack	Terrorist in ship control station getting access to the ship control systems	Terrorists gaining control over ship	6	4	10	Two or three factors authentication - Physical barrier to the control room (door, etc.) - Cameras for intrusion detection and alarm - Quick alarm to police – Alarm if cameras are lost	2	4	6
25	Collision avoidance system	Malware installation	System trying to collide with ships or specific objects	Collision/ contact/ grounding	5	4	9	Safety verification system installation / Two or three factors authentication for software modification / Firewall installation / Kernel technologies	3	2	5
27	Situation awareness system	Malware installation	Erroneous picture compilation	Collision/ contact/ grounding	5	4	9	Two or three factors authentication for software modification / Firewall installation / Kernel technologies / Intrusion detection system and Antivirus	2	4	6

5 CONCLUSIONS

The shipping industry is entering new era with autonomous vessels being designed, built and operated. However, their introduction comes at the expense of an increased number of hazardous scenarios due to potential cyber-attacks. In this paper, an enhanced CPHA was employed with the support of the FSA risk matrix for identifying the safety related cyber-attacks, which can be implemented by terrorists, to the navigation and propulsion control systems of an autonomous inland ship.

The main findings of this study are the following:

- A number of technical vulnerabilities such as GPS signal vulnerabilities, PLCs integer overflow vulnerability and VHF lack of cryptography are available at the existing systems, which can be exploited during cyber-attacks.
- Attacks on the shore control centre and the ship control station targeting at getting privileged access have the highest potential safety implications.
- Malware installation on the collision avoidance system and the situation awareness system also have significant safety implications.
- System safety can be improved by adding firewalls on the conduits between different control zones, increased redundancy in communication between control zones and installing intrusion detection systems.

This analysis results can be used to enhance autonomous and other ships designs and guide more detailed risk assessments of the ship systems. The analysis could be extended by applying the CPHA for other attack groups or supporting CPHA results by multiple expert ranking. In addition, a more detailed cyber-security analyses employing more labour intensive methods could be implemented. All this constitute suggestions for future research.

ACKNOWLEDGEMENTS

The work described in this paper was produced in research project AUTOSHIP†. The project has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No 815012. The authors greatly acknowledge the funding from DNV GL AS and RCCL for the MSRC establishment and operation. The opinions expressed herein are those of the authors and should not be construed to reflect the views of EU, DNV GL AS and RCCL.

REFERENCES

Abdulkhaleq, A., & Wagner, S. (2015). *A controlled experiment for the empirical evaluation of safety analysis techniques for safety-critical software*. Paper presented at the Proceedings of the 19th International Conference on Evaluation and Assessment in Software Engineering, Nanjing, China. http://delivery.acm.org/10.1145/2750000/2745817/a16-abdulkhaleq.pdf?ip=130.159.52.50&id=2745817&acc=ACTIVE%20SERVICE&key=C2D842D97AC95F7A%2E78A0E221B184F35C%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1517584452_9a89f171925f7a04d4c1fe9971e3675a

Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry, 100*, 212-223. Retrieved from http://www.sciencedirect.com/science/article/pii/S0166361517304244. doi:https://doi.org/10.1016/j.compind.2018.04.017

Balduzzi, M., Pasta, A., & Wilhoit, K. (2014). *A security evaluation of AIS automated identification system.* Paper presented at the Proceedings of the 30th annual computer security applications conference.

BIMCO. (2018). *Maritime Cyber Survey 2018 - the results*. Retrieved from https://webcache.googleusercontent.com/search?q=cache:rkcjvmcpCakJ:https://www.bimc

† https://trimis.ec.europa.eu/project/autonomous-shipping-initiative-european-waters

o.org/-/media/bimco/news-and-trends/news/security/cyber-security/2018/fairplay-and-bimco-maritime-cyber-security-survey-2018.ashx+&cd=1&hl=en&ct=clnk&gl=uk
Blue Lines Logistics. (2015). Blue Lines Logistics News. Retrieved from http://www.bluelinelogistics.eu/news
Bolbot, V., Theotokatos, G., Bujorianu, L. M., Boulougouris, E., & Vassalos, D. (2019). Vulnerabilities and safety assurance methods in Cyber-Physical Systems: A comprehensive review. *Reliability Engineering & System Safety, 182*, 179-193. Retrieved from http://www.sciencedirect.com/science/article/pii/S0951832018302709. doi:https://doi.org/10.1016/j.ress.2018.09.004
Borio, D., Driscoll, C. O., & Fortuny, J. (2012, 5-7 Dec. 2012). *GNSS Jammers: Effects and countermeasures.* Paper presented at the 2012 6th ESA Workshop on Satellite Navigation Technologies (Navitec 2012) & European Workshop on GNSS Signals and Signal Processing.
Code of practice - cyber security for ships, (2017).
Bozdal, M., Samie, M., & Jennions, I. (2018). *A Survey on CAN Bus Protocol: Attacks, Challenges, and Potential Solutions.* Paper presented at the 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE).
Brooks, Z. (2016). Hacking driverless vehicles. Retrieved from https://www.defcon.org/images/defcon-21/dc-21-presentations/Zoz/DEFCON-21-Zoz-Hacking-Driverless-Vehicles.pdf
BSI. (2009). Industrial communication networks. Network and system security. IEC TS 62443. In. London, United Kingdom.
CISA. (2019a). CISA - Industrial Control Systems. Retrieved from https://www.us-cert.gov/ics
CISA. (2019b). ICS Alert (ICS-ALERT-17-341-01) - WAGO PFC200. Retrieved from https://www.us-cert.gov/ics/alerts/ICS-ALERT-17-341-01
CISA. (2019c). ICS Alert (ICS-ALERT-19-211-01) - CAN Bus Network Implementation in Avionics. Retrieved from https://www.us-cert.gov/ics/alerts/ics-alert-19-211-01
CISA. (2019d). ICS Alert (ICS-ALERT-19-225-01) - Mitsubishi Electric smartRTU and INEA ME-RTU. Retrieved from https://www.us-cert.gov/ics/alerts/ics-alert-19-225-01
DNV GL. (2015). Technology outlook 2025. In.
DNV GL. (2016). DNVGL-RP-0496 - Cyber security resilience management In.
DNV GL. (2019). Part 6 Additional class notations Chapter 5 Equipment and design features Section 21 Cyber security. In D. GL (Ed.), *Part 6 Chapter 5 Section 21*.
Eloranta, S., & Whitehead, A. (2016). *Safety aspects of autonomous ships*. Paper presented at the 6th International Maritime Conference, Germany, Hamburg.
Farid, M. A., Ahmad, M., Ahmed, S., & Rahim, S. S. (2018). Impact and detection of GPS jammers and countermeasures against jamming. *International Journal of Scientific & Engineering Research, 9*(12), 47-54.
Flaus, J.-M. (2019). *Cybersecurity of industrial systems*. London, United Kingdom: ISTE Ltd.
Goward, A. (2017). Mass GPS Spoofing Attack in Black Sea? Retrieved from https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea
Höyhtyä, M., Huusko, J., Kiviranta, M., Solberg, K., & Rokka, J. (2017). *Connectivity for autonomous ships: Architecture, use cases, and research challenges.* Paper presented at the 2017 International Conference on Information and Communication Technology Convergence (ICTC).
Hussain, S., Chowdhury, O., Mehnaz, S., & Bertino, E. (2018). *LTEInspector: A systematic approach for adversarial testing of 4G LTE.* Paper presented at the Network and Distributed Systems Security (NDSS) Symposium 2018.
IEC. (2011a). IEC 27005 - Information technology - security techniques - Information security risk management. In.
IEC. (2011b). Information technology — Security techniques — Information security risk management - ISO 27005. In. Switzerland: International Standard organisation.
IMO. (2016). Interim guidelines on maritime cyber risk management. In *MSC.1-CIRC.1526* (pp. 6).
International Maritime Organisation. (2013). *Revised guidelines for formal safety assessment (FSA) for use in the IMO rule-making process*. London Retrieved from http://research.dnv.com/skj/IMO/MSC-MEPC%202_Circ%2012%20FSA%20Guidelines%20Rev%20III.pdf

Jones, K. D., Tam, K., & Papadaki, M. (2016). Threats and impacts in maritime cyber security.
Kang, T. U., Song, H. M., Jeong, S., & Kim, H. K. (2018). *Automated Reverse Engineering and Attack for CAN Using OBD-II.* Paper presented at the 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall).
Kavallieratos, G., Katsikas, S., & Gkioulos, V. (2019, 2019//). *Cyber-Attacks Against the Autonomous Ship.* Paper presented at the Computer Security, Cham.
Krotofil, M., C, A. A., #225, rdenas, Manning, B., & Larsen, J. (2014). *CPS: driving cyber-physical systems to unsafe operating conditions by timing DoS attacks on sensor signals*. Paper presented at the Proceedings of the 30th Annual Computer Security Applications Conference, New Orleans, Louisiana, USA. http://delivery.acm.org/10.1145/2670000/2664290/p146-krotofil.pdf?ip=130.159.52.50&id=2664290&acc=ACTIVE%20SERVICE&key=C2D842D97AC95F7A%2E78A0E221B184F35C%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1517585100_9ccf2acc8cc4da601c49f53468c4c434
Lund, M. S., Hareide, O. S., & Jøsok, Ø. (2018). An attack on an integrated navigation system.
Cyber security Assessment and protection of ships, (2016).
Munro, K. (2017). OSINT from ship satcoms. Retrieved from https://www.pentestpartners.com/security-blog/osint-from-ship-satcoms/
Nazir, S., Patel, S., & Patel, D. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security, 70*, 436-454. Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404817301293. doi:https://doi.org/10.1016/j.cose.2017.06.010
NIST. (2019). National vulnerability database. Retrieved from https://nvd.nist.gov/vuln
Oates, R., Roberts, J., & Twomey, B. (2017). *Chains, links and lifetime: Robust security for autonomous maritime systems*. Paper presented at the Marine Electrical and Control Systems Safety, Glasgow, United Kingdom.
Omitola, T., Downes, J., Wills, G., Zwolinski, M., & Butler, M. (2018). Securing navigation of unmanned maritime systems.
Schmidt, M., Fentzahn, E., Atlason, G. F., & Rødseth, H. (2015). *D8.7: Final report: Autonomous engine room*. Retrieved from
Shinohara, T., & Namerikawa, T. (2017). On the vulnerabilities due to manipulative zero-stealthy attacks in cyber-physical systems. *SICE Journal of Control, Measurement, and System Integration, 10*(6), 563-570.
Stefani, A. (2013). *An introduction to ship automation and control systems*. United Kingdom, London: Institute of Marine Engineering, Science & Technology.
Tam, K., & Jones, K. (2018). *Cyber-risk assessment for autonomous ships.* Paper presented at the 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security).
Tam, K., & Jones, K. (2019). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs, 18*(1), 129-163. Retrieved from https://doi.org/10.1007/s13437-019-00162-2. doi:10.1007/s13437-019-00162-2
Cyber strategy, (2015).
Wingrove, M. (2018). 'Impregnable' radar breached in simulated cyber attack. Retrieved from https://www.rivieramm.com/news-content-hub/impregnable-radar-breached-in-simulated-cyber-attack-25158
Young, W., & Leveson, N. G. (2014). An integrated approach to safety and security based on systems theory. *Communnications of the ACM, 57*(2), 31-35. Retrieved from http://delivery.acm.org/10.1145/2560000/2556938/p31-young.pdf?ip=130.159.52.50&id=2556938&acc=ACTIVE%20SERVICE&key=C2D842D97AC95F7A%2E78A0E221B184F35C%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1517585608_c8f755bbec0c78ad166f12fbd04cf307. doi:10.1145/2556938

APPENDIX A – ABBREVIATION LIST

AIS	Automatic Identification System
CISA	Cybersecurity and Infrastructure Security Agency
CPHA	Cyber Preliminary Hazard Analysis
DoS	Denial of Service
ECDIS	Electronic Chart Display Information System
FSA	Formal Safety Assessment
GMDSS	Global Maritime Distress and Safety System
GPS	Global Positioning System
LADAR	Laser Detection And Ranging
LiDAR	Light Detection And Ranging
MaCRA	Maritime Cyber-Risk Assessment
PHA	Preliminary Hazard Analysis
PLC	Programmable Logic Controller
PSB	Pallet Shuttle Barge
RADAR	RAdio Detection And Ranging
SCADA	System Control And Data Acquisition
VDR	Voyage Data Recorder
VHF	Very High Frequency